The Importance of International Coordination and Collaboration from a Vender's Perspective

By

Samuel M. Smith Ph.D.

August 10, 2006

Adept Systems Inc.,

2966 Fort Hill Road Utah 84005

801.766.3527x112 (voice) 801.766.3528 (fax)

smithsm@adeptsystemsinc.com   www.adeptsystemsinc.com,

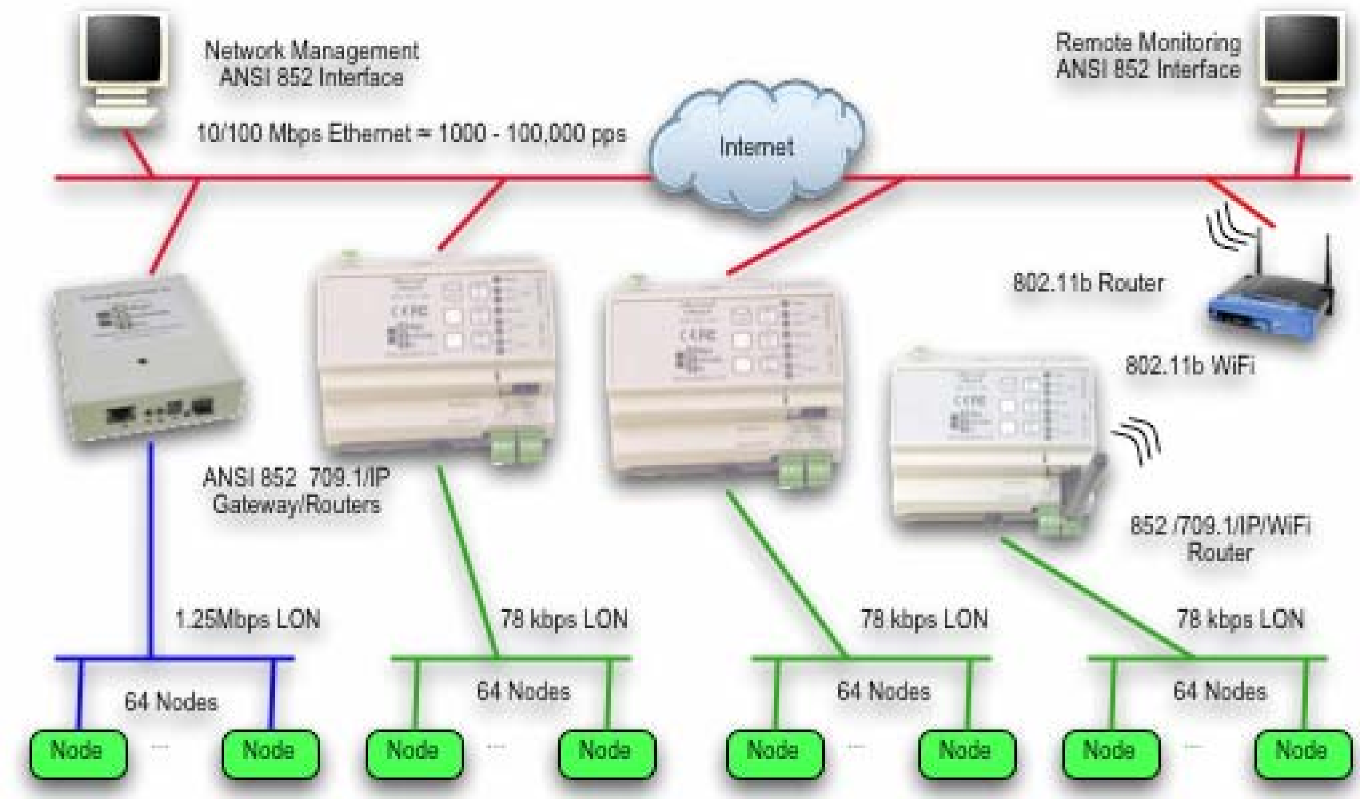
Adept Systems Inc.

Adept founded in 1994

- Experts in networked automation & control systems
- Expertise in ANSI 709.1/ 852 & IEEE 1394 protocols
- Active participant in ANSI 709.1, 852, 852.1 standards development
- Expertise in engineering design, vertical capability for embedded systems, software, electronics design and manufacture

Adept's Role

- OEM of Standards Based Component Level Automation Infrastructure (CLAI) components for worldwide market
- Technology Innovator
- Developer of prototypes and capability demonstrations
- Research and Development in systems design for survivability and affordability



International Standards Dependency

- Adept would not have a business without standards
  - ANSI/EIA/CEA 709.1, 709.2, 709.3,
  - ANSI/EIA/CEA 852A 852.1
  - CENELEC TC247 - EN 14908.1, 14908.2, 14908.3, 14908.4, 14908.5
  - ISO/IEC JTC-1/SC25 WG#1
  - LONMark
  - IEEE 802.11, 802.3
  - EIA 485
  - CE mark
  - FCC EMI
  - ROHS
  - Web Standards
  - OBIX
- Standards management is single largest external business management activity
  - Committees, coordination, collaboration
  - Implementation development and testing
  - Manufacturing compliance
  - Advance marketing, education, and awareness

CN/IP Tunneling

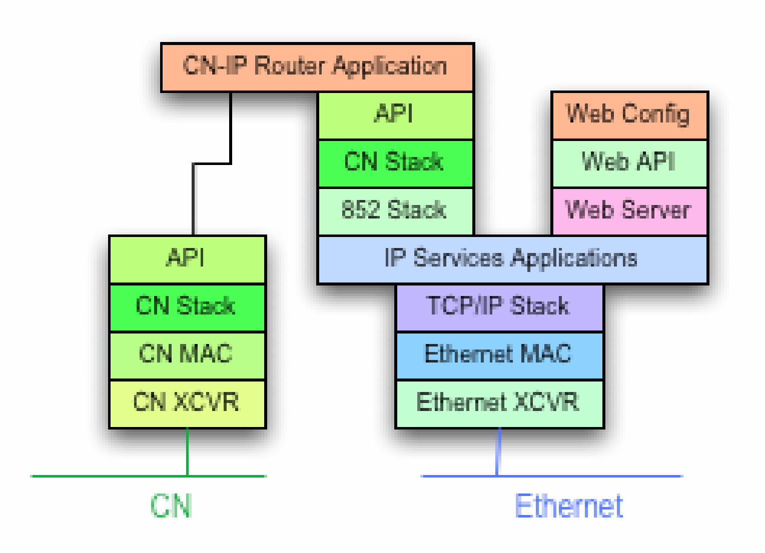
- Building Management Systems: HVAC, Lighting, Security, Utilities
  - Leverage IP networks, CN wiring expensive
  - Remote monitoring and management
  - Enterprise Integration
  - Newer systems no longer isolated
- Component Network (CN)
  - Device level protocol such as LonTalk, CAN, CEBus, Profibus, BacNet …
- IP Tunneling with CN-IP Gateways
  - Source CN-IP Gateway adds IP Header “wrapper” to CN packet received from source CN Node
  - Source CN-IP Gateway delivers wrapped packet over IP network to destination IP-CN Gateway
  - Destination IP-CN Gateway removes IP Header and delivers CN packet to destination CN node
- Need IP Management Layer on Top of CN
  - IP addressing
- CN-IP Device Types
  - CN Router (Network Layer Gateway)
  - CN Node that communicates using IP only (direct tunneling with gateway)
  - Application Layer Gateway
- Example IP Tunneling Protocols
  - ANSI 852 “LonTalk”,ProfiNet, BacNet/IP

ANSI 852, Cenelec EN14908.4 Standard

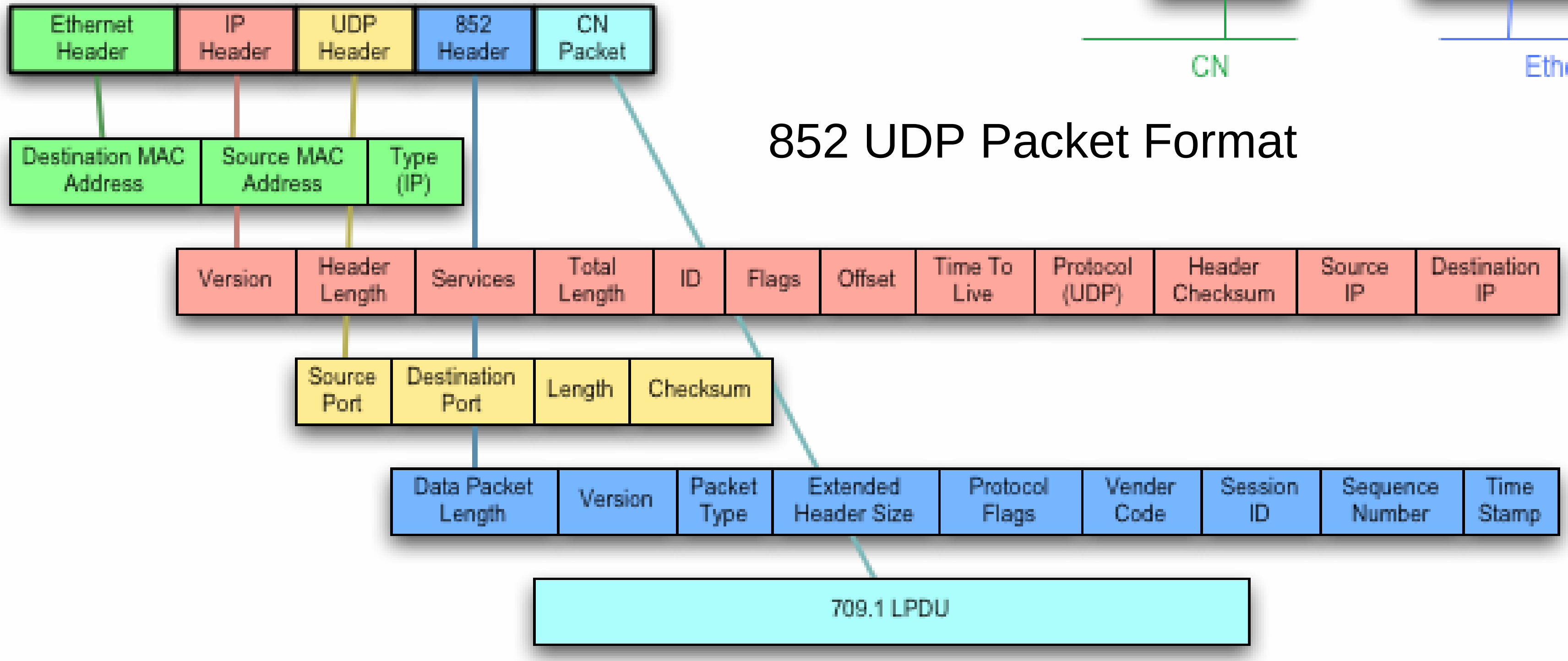
- 852 (2001), 852-A (2004)
  - Generic Configuration Protocol for IP Tunneling of Component Networks
  - Application Level Interface for Configuration Services. Manual or Automatic
  - CN Packet Order Preserving
  - Packet Aggregation and Segmentation
  - Duplicate and Stale Packet Handling
  - MD5 Packet Authentication for Security, no encryption
    - Additional CN Security or Authentication Schemes
  - Uni-cast or Multi-cast, UDP or TCP
  - Selective Forwardiing
- 852.1 (In Development)
  - Enhanced Configuration Management for Scalability
  - Optimized Forwarding Algorithm
  - NAT
  - Virtual Configuration Servers
  - Bilingual Interoperability Path
  - Notably missing so far is enhanced security
- 852.1A
  - IPV6
  - Data Encryption

852 CN Router/IP Gateway

CN/IP Router/Gateway Architecture


CN-IP Router Application
API
CN Stack
852 Stack
Web Config
Web API
Web Server
IP Services Applications
API
CN Stack
CN MAC
CN XCVR
TCP/IP Stack
Ethernet MAC
Ethernet XCVR
CN
Ethernet

852 UDP Packet Format


Ethernet Header | IP Header | UDP Header | 852 Header | CN Packet

Destination MAC Address | Source MAC Address | Type (IP)

Version | Header Length | Services | Total Length | ID | Flags | Offset | Time To Live | Protocol (UDP) | Header Checksum | Source IP | Destination IP

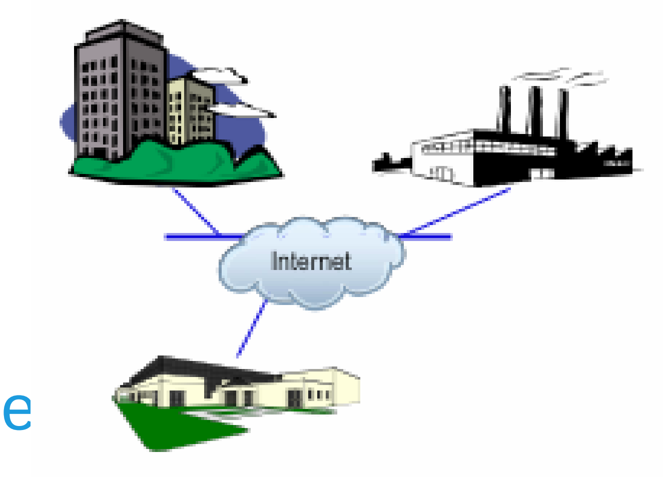
Source Port | Destination Port | Length | Checksum

Data Packet Length | Version | Packet Type | Extended Header Size | Protocol Flags | Vender Code | Session ID | Sequence Number | Time Stamp

709.1 LPDU

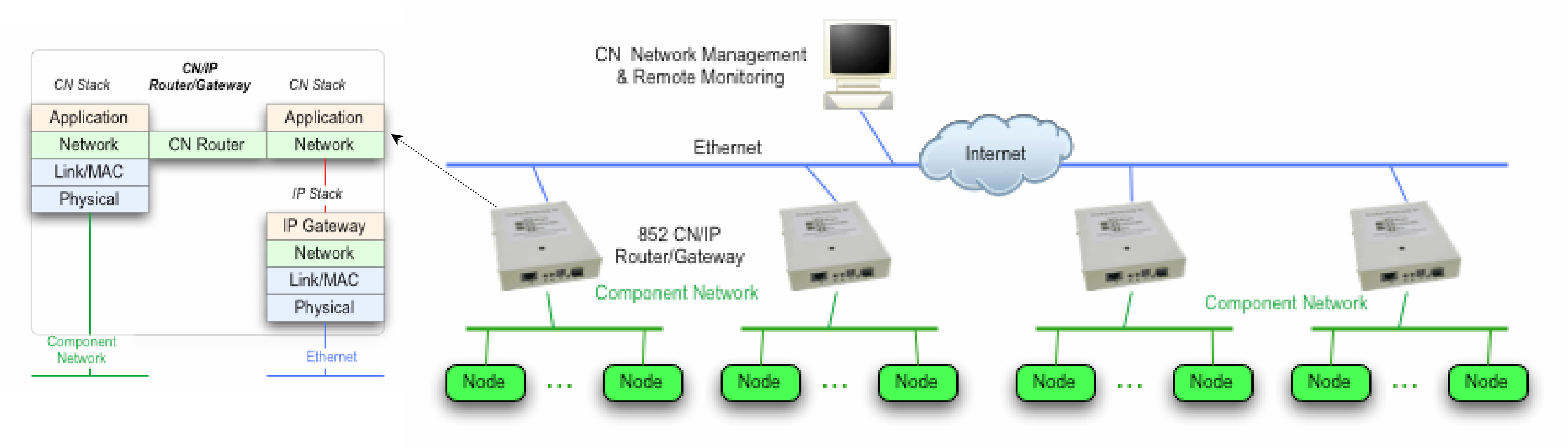
Systems Integration Problems

- Building Large CN Networks
  - Large number of nodes
  - Bandwidth Management
  - Distributed over Multiple sites
  - Leverage Existing IP Network Infrastructure
  - Retrofit



- High Availability Applications
  - Redundancy

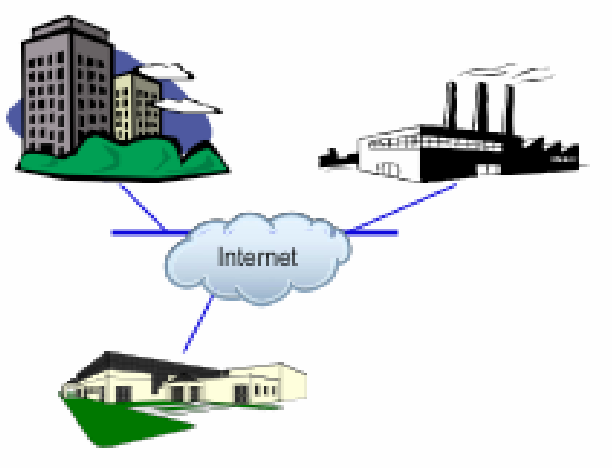
852 Standard Based “Transparent” CN/IP Router/Gateway

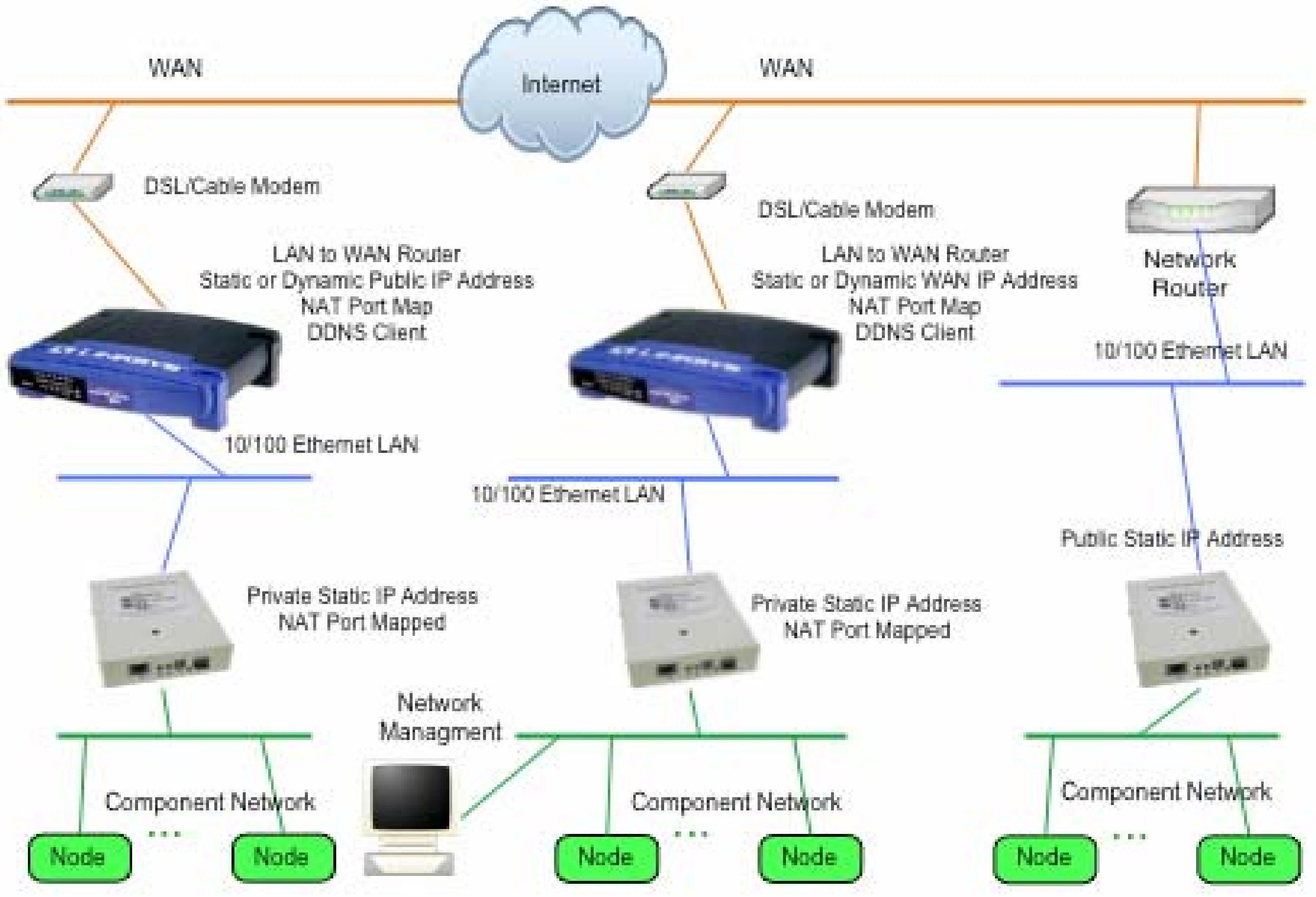


Advantages:

Transparent “Flat Architecture”
Unified Network Management
High Performance
Scalable
Enables Remote Monitoring
Enables Hybrid Architectures

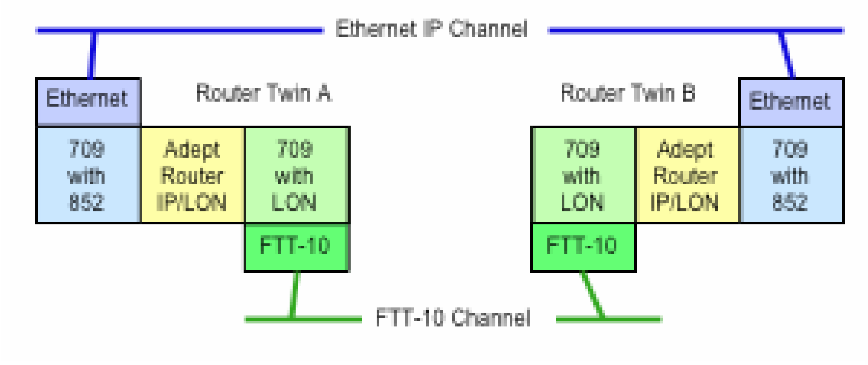
NAT and DDNS

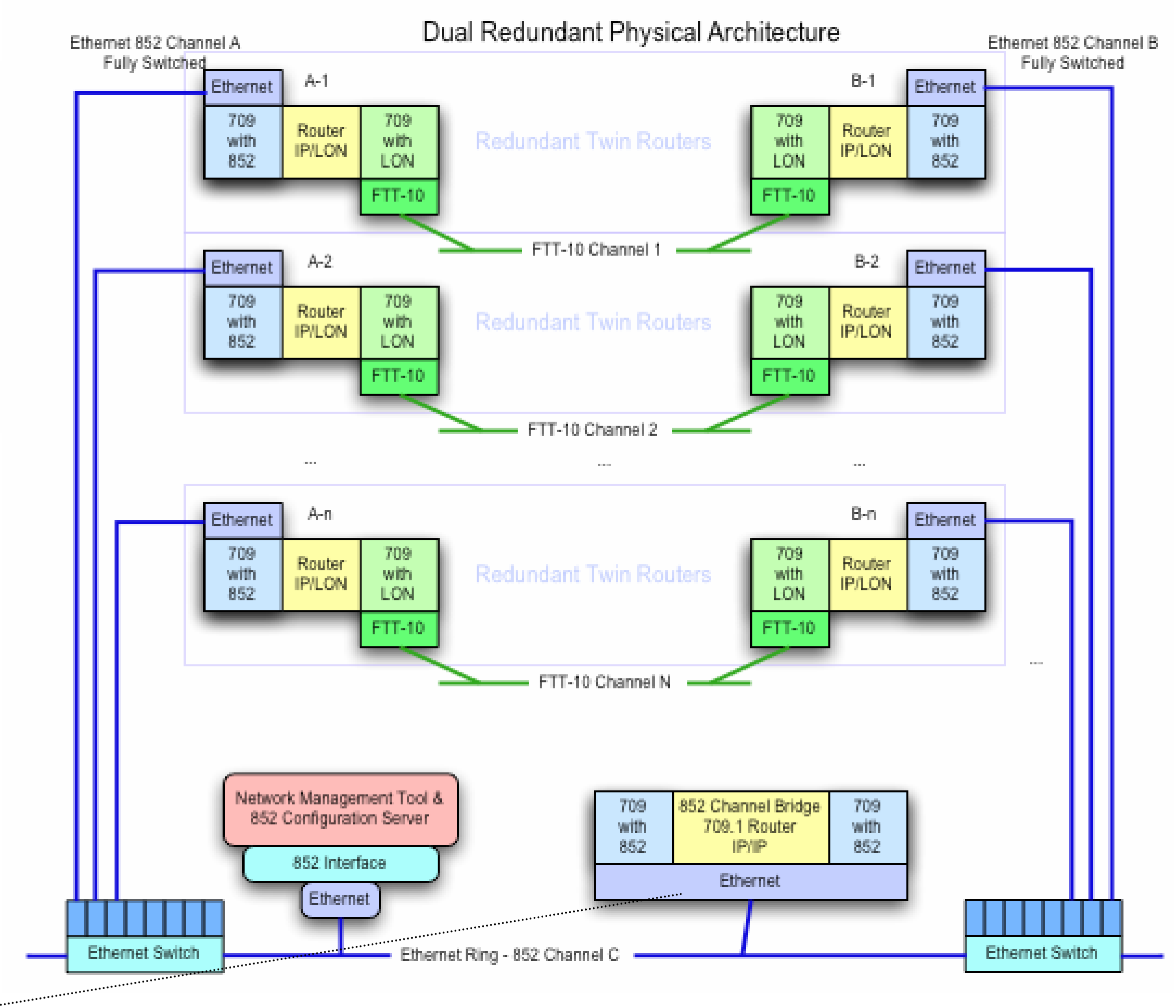

Internet

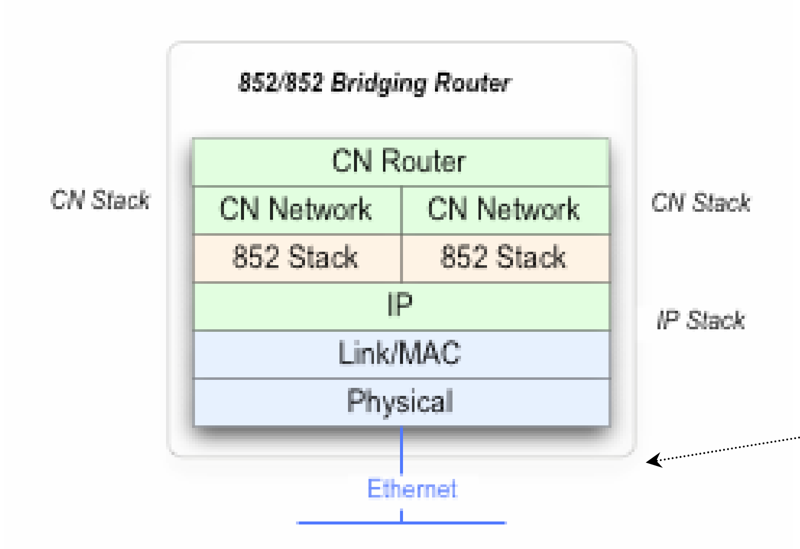

WAN
Internet
WAN
DSL/Cable Modem
DSL/Cable Modem
LAN to WAN Router
Static or Dynamic Public IP Address
NAT Port Map
DDNS Client
LAN to WAN Router
Static or Dynamic WAN IP Address
NAT Port Map
DDNS Client
Network
Router
10/100 Ethernet LAN
10/100 Ethernet LAN
10/100 Ethernet LAN
Public Static IP Address
Private Static IP Address
NAT Port Mapped
Private Static IP Address
NAT Port Mapped
Network
Managment
Component Network
Component Network
Component Network
Node
...
Node
Node
...
Node
Node
...
Node

High Availability Architecture

Dual Redundant CN/IP Routers







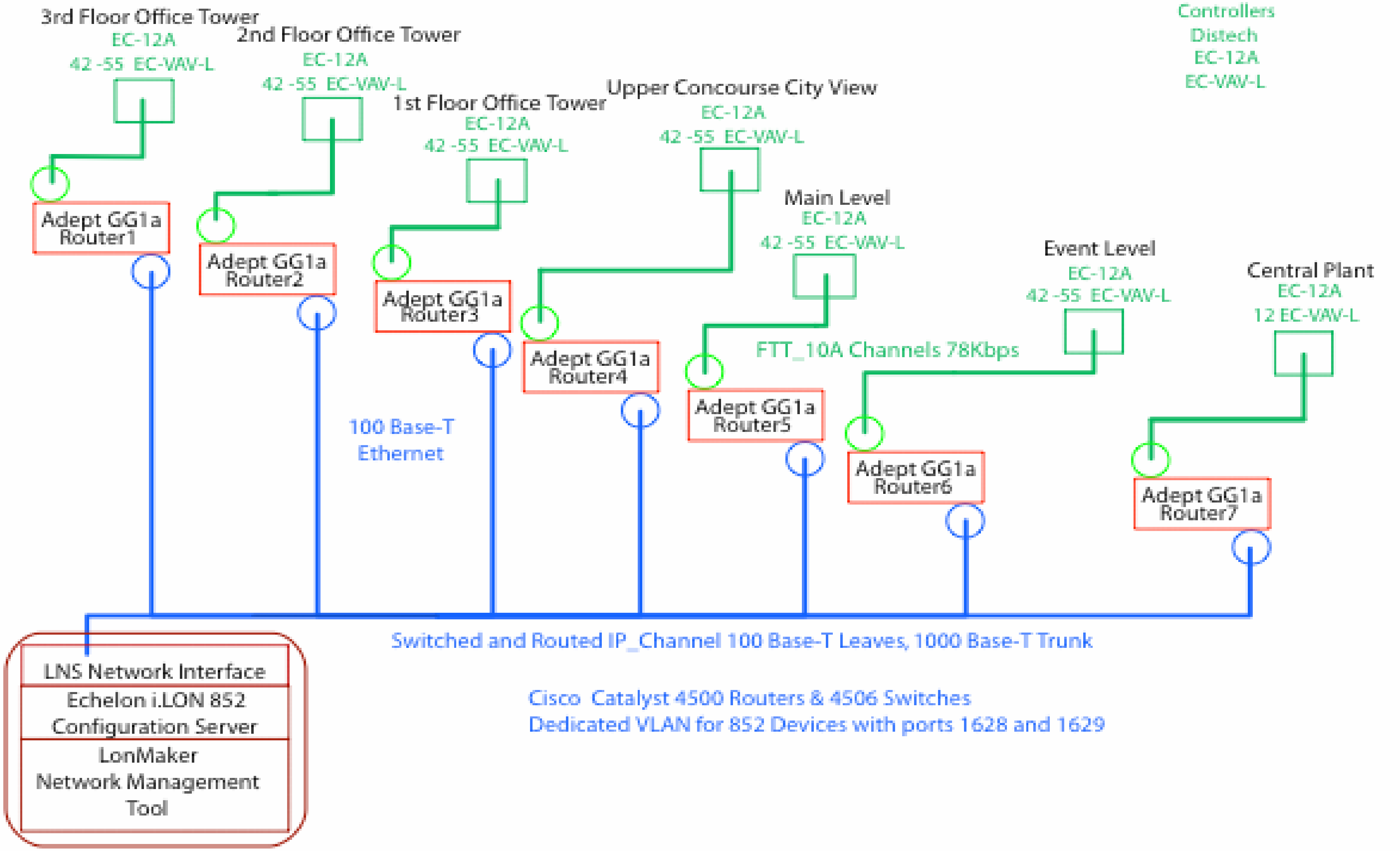
Adept Systems Inc

Case Studies

- Stadium “Staples Center”
- High Availability “Pharmaceutical Plant”
- High Availability “Automated Fire Suppression System”

Staples Center Network

“852/IP backbone was phenomenally more responsive than the 1250 backbone”.



Controllers
Distech
EC-12A
EC-VAV-L

3rd Floor Office Tower
EC-12A
42 -55 EC-VAV-L

2nd Floor Office Tower
EC-12A
42 -55 EC-VAV-L

1st Floor Office Tower
EC-12A
42 -55 EC-VAV-L

Upper Concourse City View
EC-12A
42 -55 EC-VAV-L

Main Level
EC-12A
42 -55 EC-VAV-L

Event Level
EC-12A
42 -55 EC-VAV-L

Central Plant
EC-12A
12 EC-VAV-L

FTT_10A Channels 78Kbps

Adept GG1a Router1

Adept GG1a Router2

Adept GG1a Router3

Adept GG1a Router4

Adept GG1a Router5

Adept GG1a Router6

Adept GG1a Router7

100 Base-T
Ethernet

Switched and Routed IP_Channel 100 Base-T Leaves, 1000 Base-T Trunk

LNS Network Interface

Echelon i.LON 852
Configuration Server

LonMaker
Network Management
Tool

Cisco Catalyst 4500 Routers & 4506 Switches
Dedicated VLAN for 852 Devices with ports 1628 and 1629

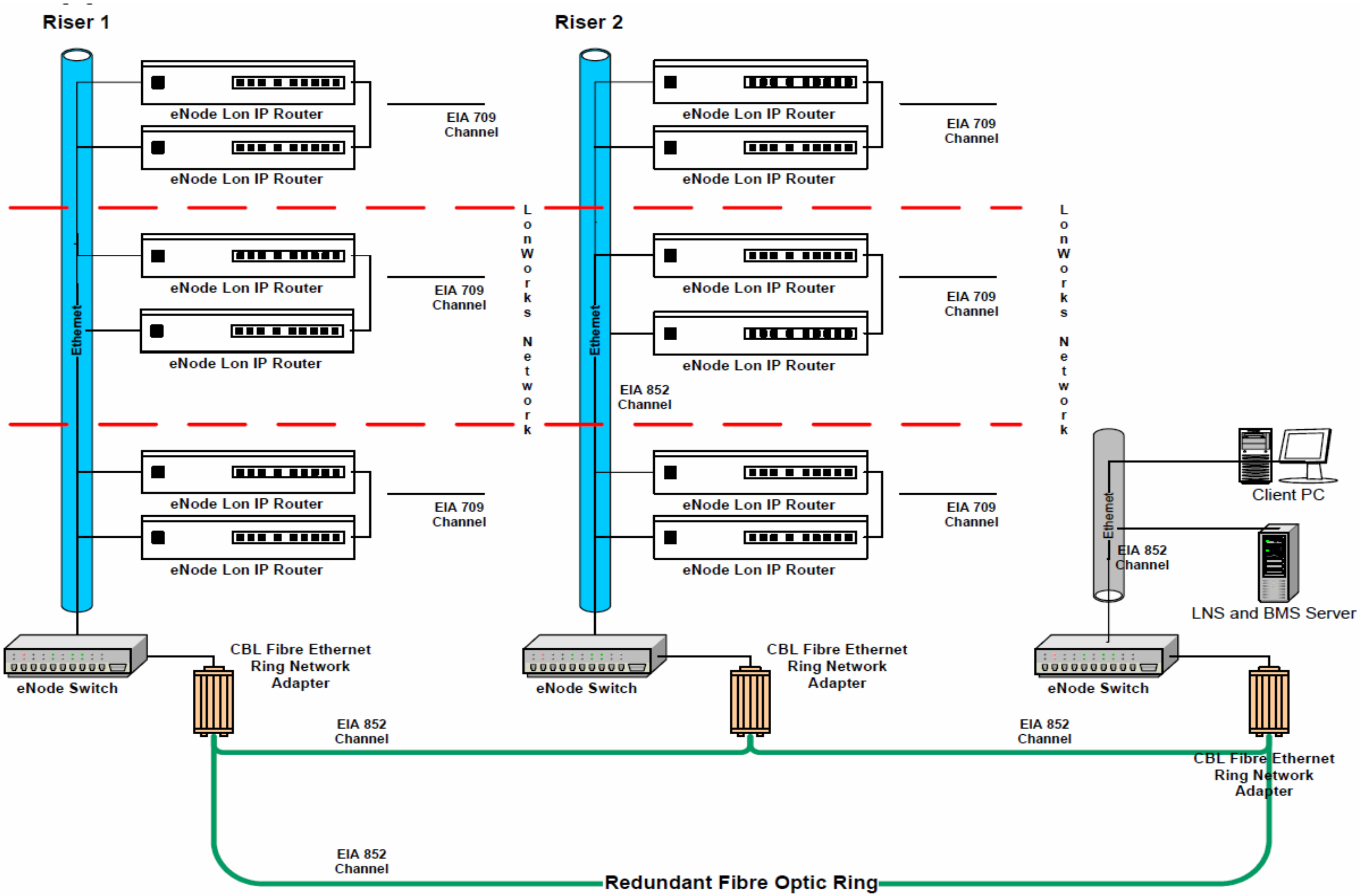
Pharmaceutical Plant

- Needed highly reliable 709.1/852 network
  - Minimize single point failure sources
  - Fully redundant network infrastructure although not redundant control devices
- Solution
  - FTT-10 Rings
  - Dual Redundant 100 Base-T Ethernet
  - Fiber Ethernet Redundant Ring
  - Redundant Twin Mode LON/IP routers
  - 30 Routers 15 FT-10 channels in Phase 1
- 709.1/852 Network Team
  - TAC UK
  - Control Network Solutions
  - Adept Systems

QuickTime™ and a
TIFF (Uncompressed) decompressor
are needed to see this picture.

QuickTime™ and a
TIFF (Uncompressed) decompressor
are needed to see this picture.

High Availability Plant



AFSS on EX USS Shadwell

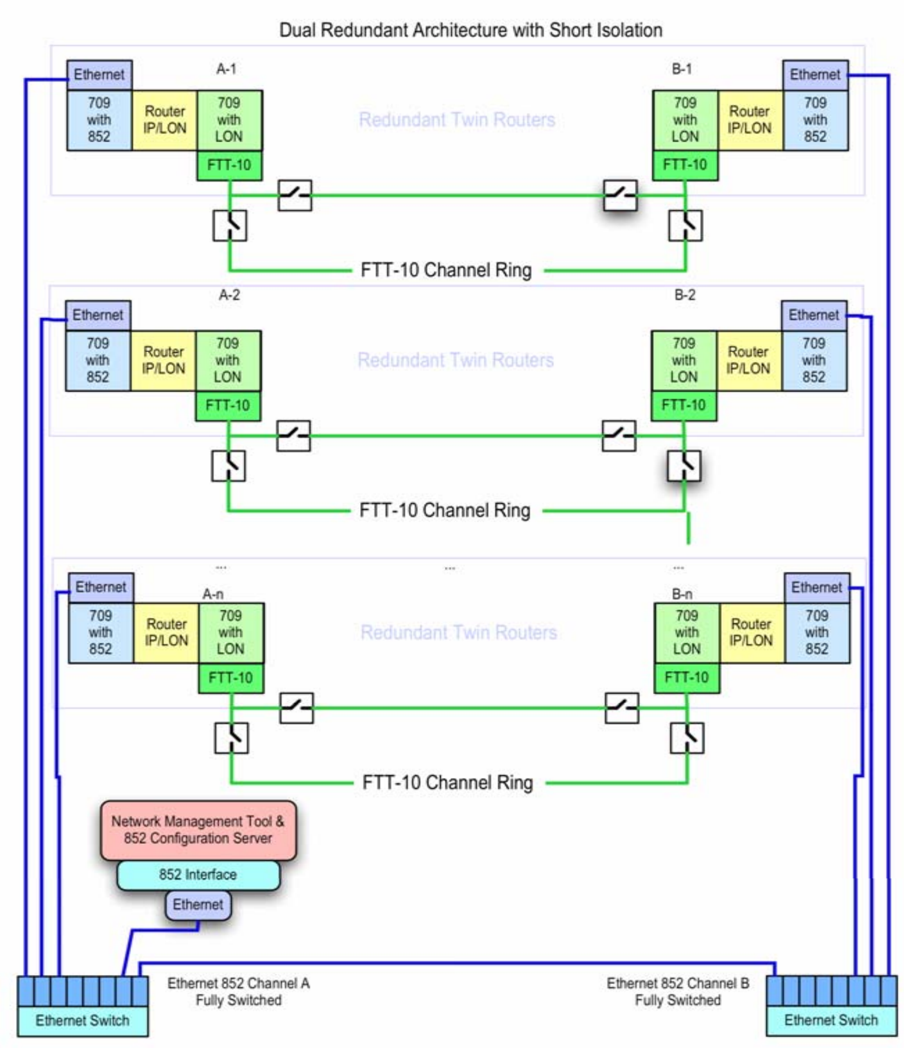
- Naval Surface Warfare Center (Philadelphia)
- Survivable Automated Fire Suppression System
  - Test on EX USS Shadwell
  - 709.1 and 852 Based
  - FTT-10 Rings
  - IP Backbone with Redundant Twin LON IP Routers
  - Smart FTT-10 Short Isolators
  - Smart Valves

Naval Surface Warfare Center
Carderock Division

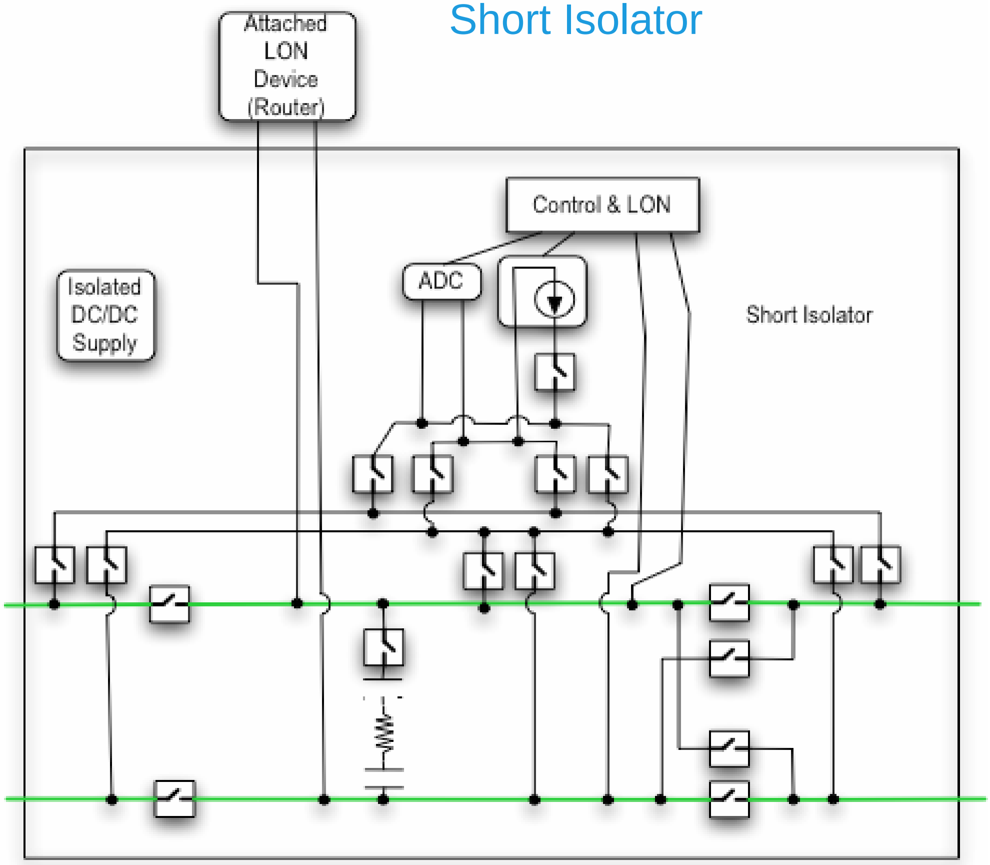
NAVSEA
NAVAL SEA SYSTEMS COMMAND

QuickTime™ and a
TIFF (Uncompressed) decompressor
are needed to see this picture.

AFSS Test Network


Dual Redundant Architecture with Short Isolation
A-1
B-1
Ethernet
709 with 852
Router IP/LON
709 with LON
FTT-10
Redundant Twin Routers
FTT-10 Channel Ring
A-2
B-2
...
A-n
B-n
Network Management Tool & 852 Configuration Server
852 Interface
Ethernet
Ethernet 852 Channel A Fully Switched
Ethernet 852 Channel B Fully Switched
Ethernet Switch

Short Isolator



CN/IP Tunneling Vulnerabilities

- Malicious Configuration Server Hijack
  - Configuration without authentication may make a device susceptible to being hijacked by malicious configuration server
- Malicious Device Masquerade
  - Configuration without authentication may allow malicious device to masquerade as legitimate device and be allowed to join channel
- Malicious Intercept and Replace of Tunneled Packets
  - CN tunneled packets sent without authentication may be intercepted and replaced with malicious packets as long as CN packets are not also authenticated
- Denial of Service Attacks

Lessons Learned From Survivability

- How to make automation systems more survivable to catastrophe ***cost-effectively?***
- Survivability: Three Aspects
  - Susceptibility = *Likelihood of strike*
  - Vulnerability = *Ease of damage once hit*
  - Recoverability = *Ease of repair once damaged*
- Damage will Occur, no matter what. Hardening is an exercise in diminishing returns.
  - Dynamic Reconfigurability is the Key.
  - xN+M Redundancy
  - Avoid common mode failures
  - Slow down damage propagation, buy time to respond

Control System Specific Characteristics

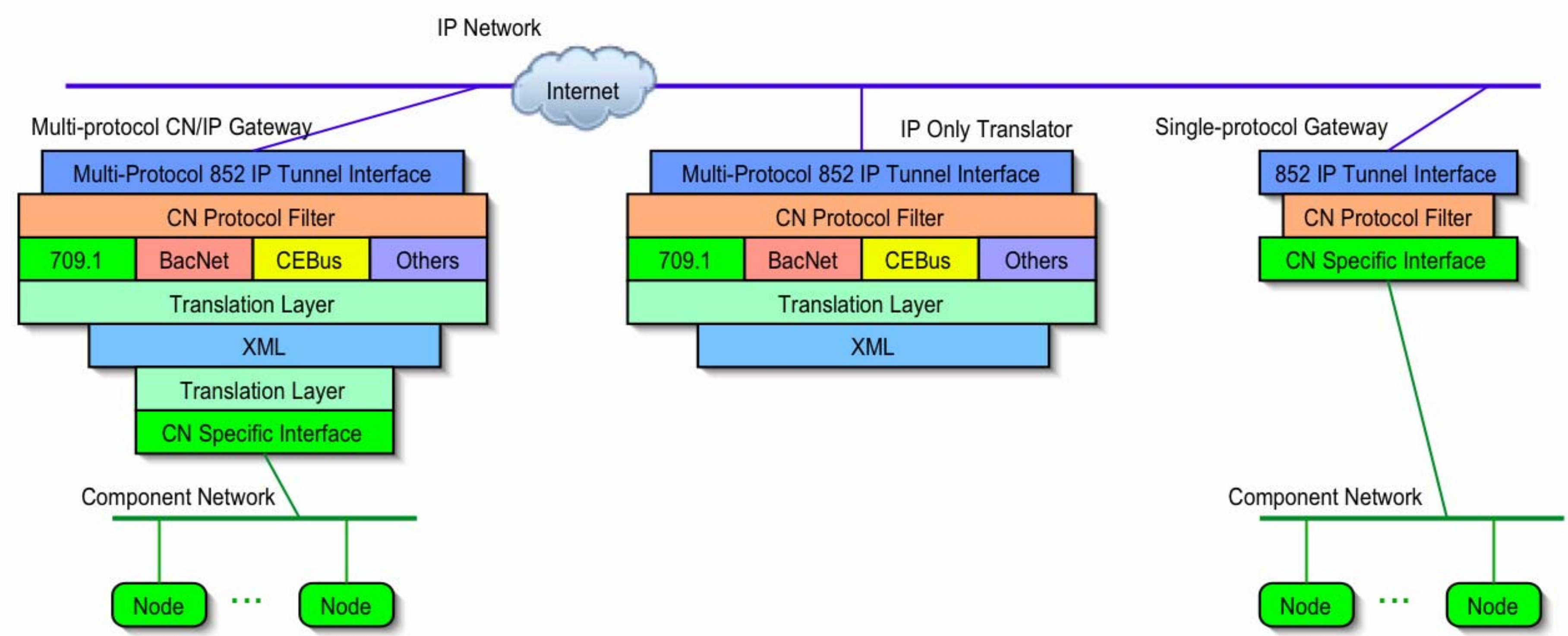
- Well known expected behavior, easier to detect failure or misbehavior
- Integral feedback loops can be used to compensate for malicious input.
- Redundancy associated with high availability systems. Provides opportunity to recover

Keys to Solution

- Dependable Topologies
- Local Intelligence
- Dynamically Reconfigurable Systems
- Modularity, Interoperability, Distributibility

Future

- Interoperable Multi-Protocol 852 CN/IP Gateways
  - Simplified Multi-protocol systems integration, configuration, and management.
  - Enabling Infra-structure for protocol and data translation
  - Protocol conversion at the network layer for transparency

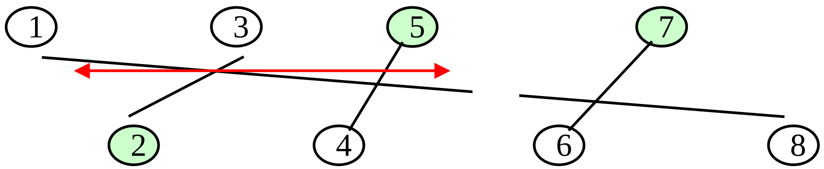


Background

Network Topologies

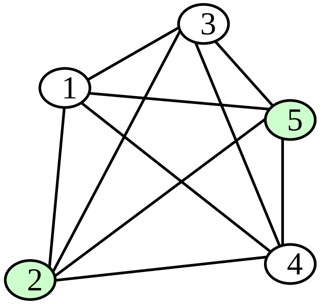
BUS

Single Point Failure Susceptable



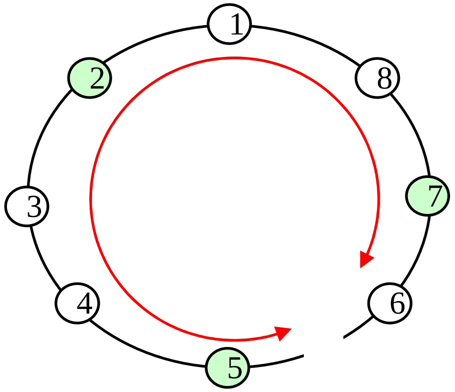
MESH

Multiple Point Failure Tolerant
Not Scalable



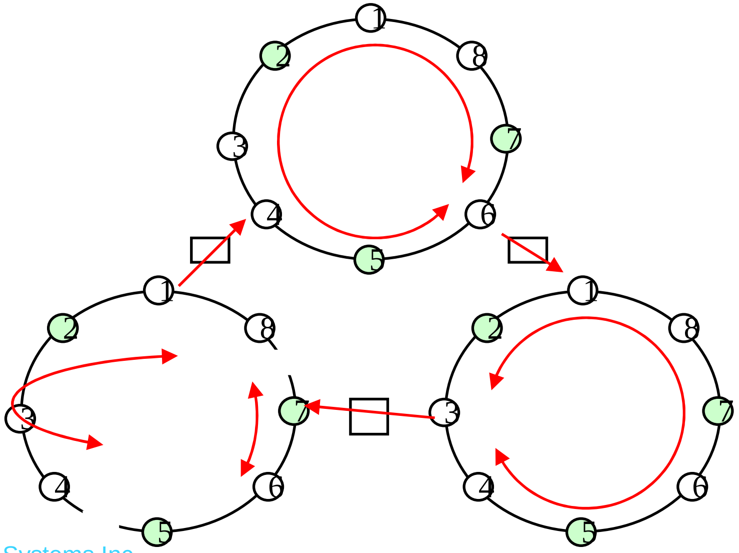
RING

Single Point Failure Tolerant



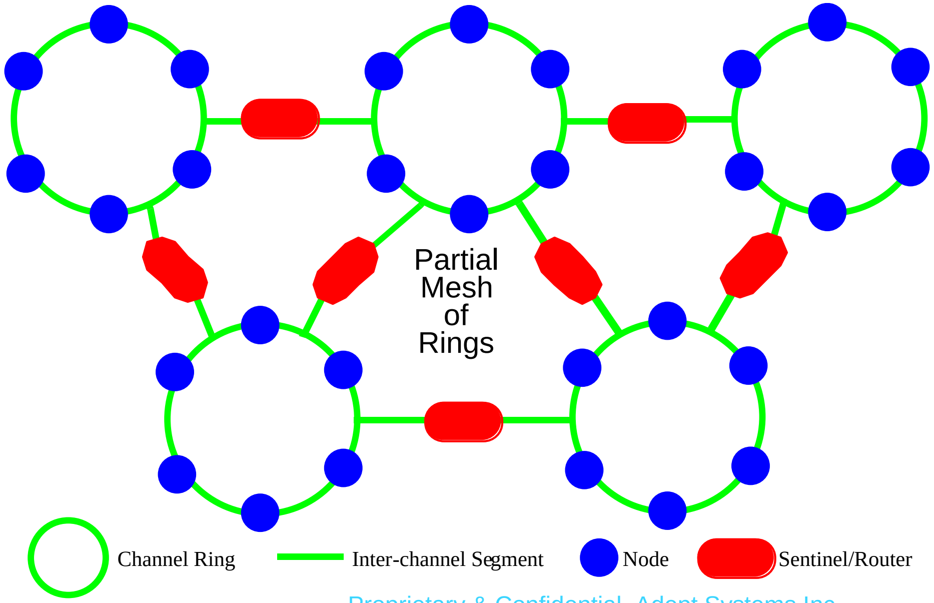
HYBRID

Multiple Point Failure Tolerant
Scalable



Dependable Network Characteristics

- Provides reliable communications in the presence of noise, malfunctioning nodes, and high traffic loads
- Does not suffer any interruption in network traffic due to single point media failures.
- Provides reliable delivery of packets at acceptable latencies
- Detects and reports single point failures
- Detects and reports multiple point failures
- Has redundant paths to reroute around network failures either single or multiple
- Can restore fragment operation through activation of redundant components



LonTalk Uniquely Suited for Reconfigurable Wired "Field Bus"

- LonTalk provides routing capability and large address space
- LonTalk supports multiple media types and tunneling
- LonTalk supports reliable message delivery
- FTT-10 supports "ring" topologies
- Multi-vendor interoperability
- Army Corp of Engineers standard for building automation

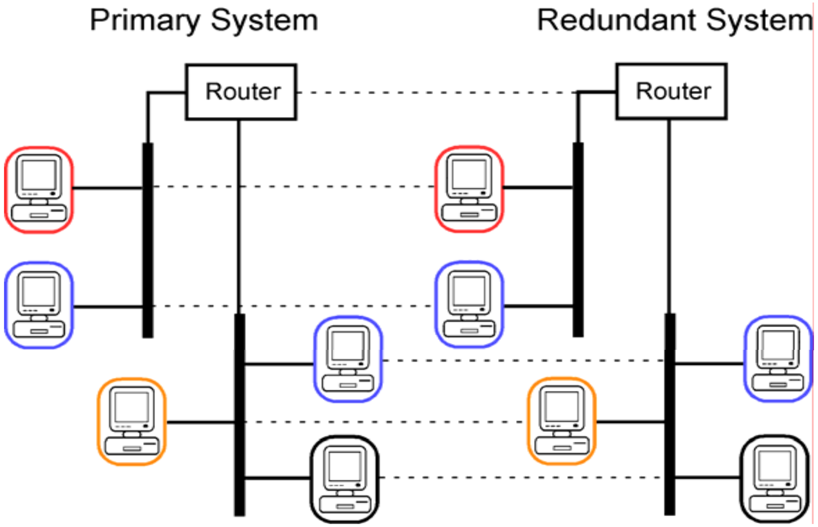
Fault Tolerance Redundancy Schemes

xN Redundancy: x copies of the system (order N)

- Simplified fault management protocol
- Inherently Unscalable
- Cost Factors Scale Non-linearly with x
- Connectivity Problems

2N : 1

System Copy

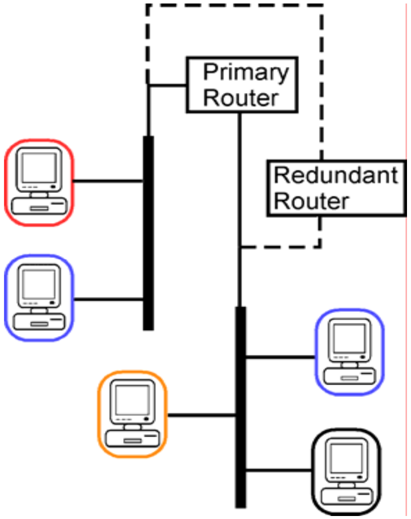


xN+m Redundancy: m copies of reconfigurable critical components

- Robust fault management protocol
- Scale logistically with network
- Scale economically with network

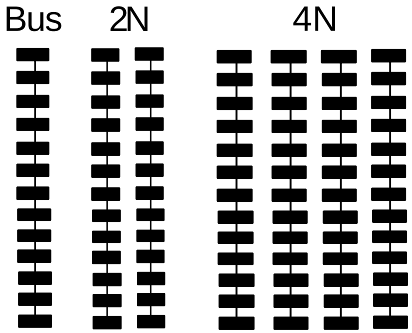
N + 1:

Router Backup

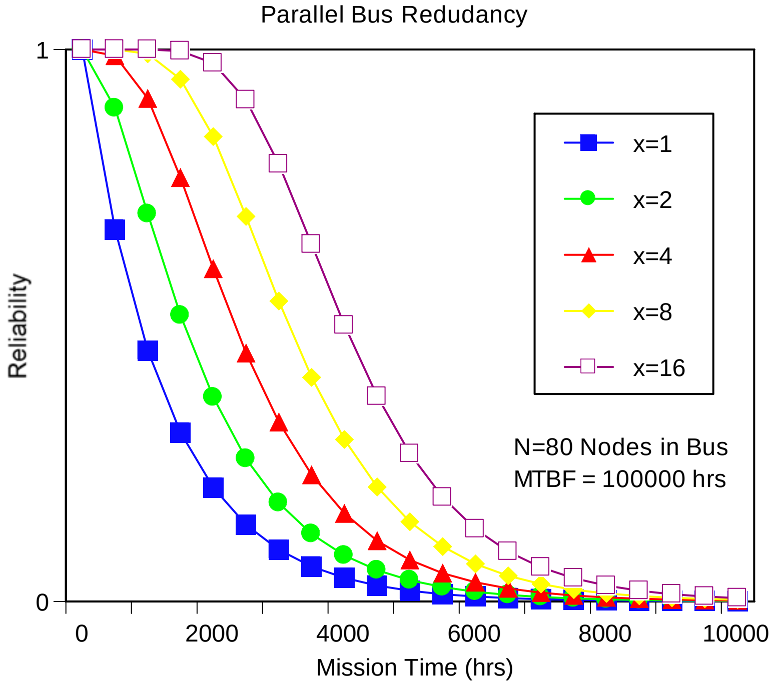


xN+ m Redundancy

xN Redundancy:
80 node bus:

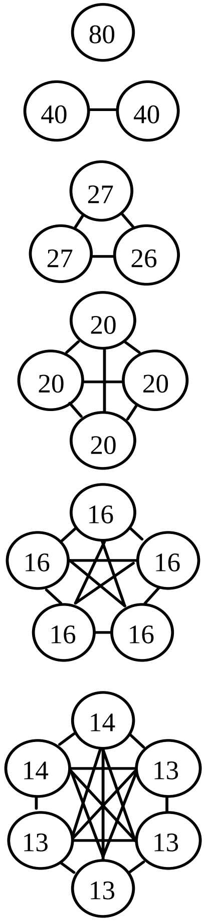


Exponential increase in hardware:
x = 2, 4, 8, 16. (x copies of N nodes)
Linear increase in Reliability

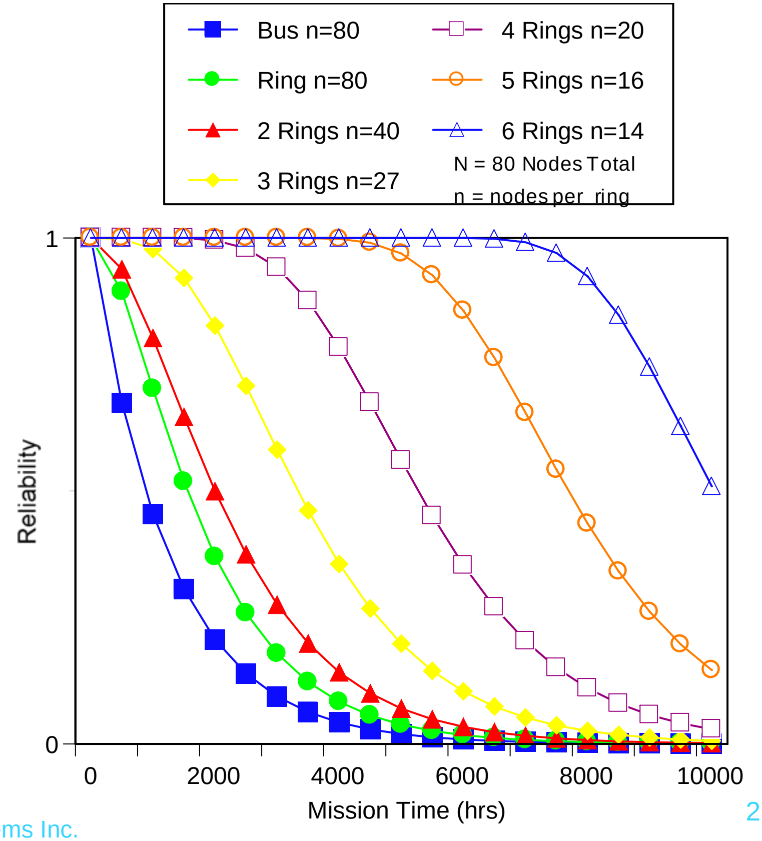


N=80 Nodes in Bus
MTBF = 100000 hrs

xN+ m Redundancy:
80 Nodes partial mesh of channels

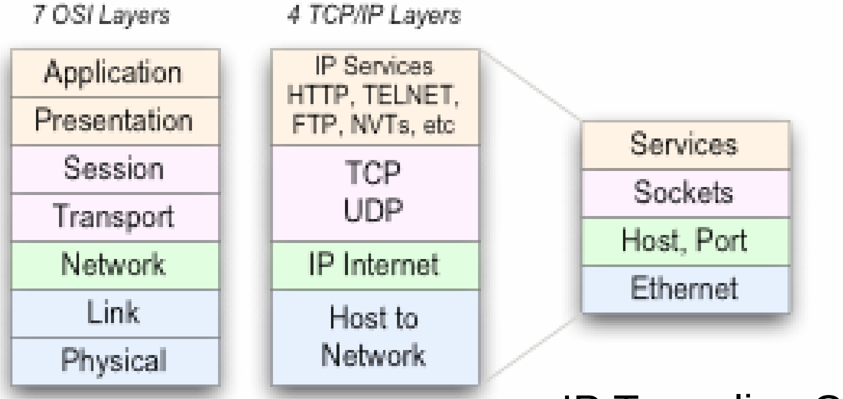


Fractional increase in hardware:
m = 1, 3, 6, … (m redundant routers)
Exponential increase in Reliability
Enables optimized reliability vs. cost

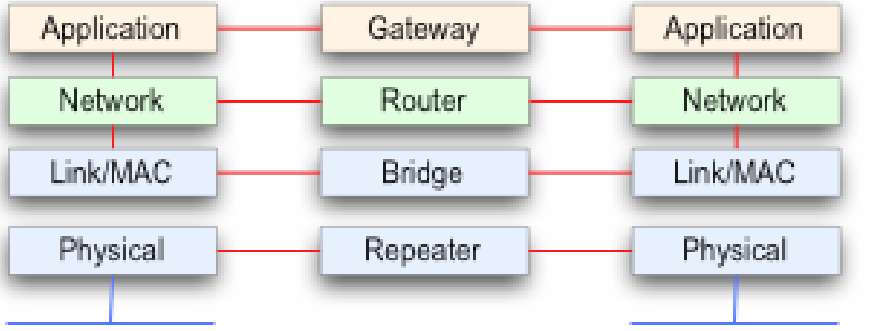


Network Component Terminology

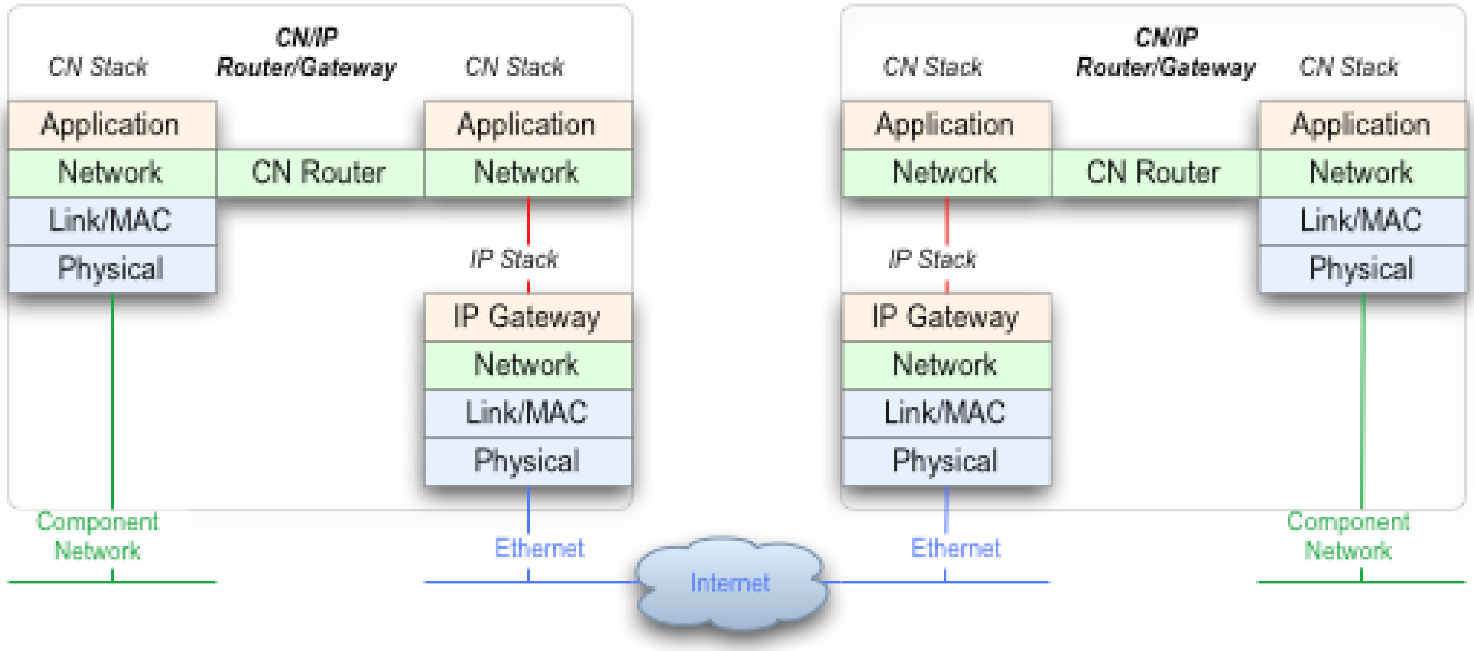
Protocol Reference Models



Network Connectors



IP Tunneling Connector

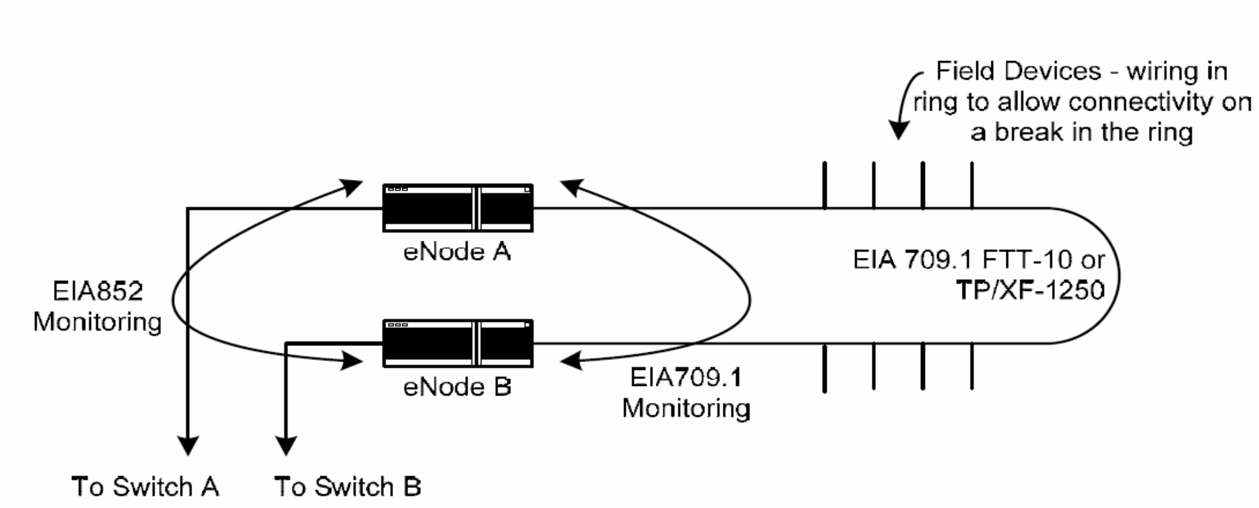


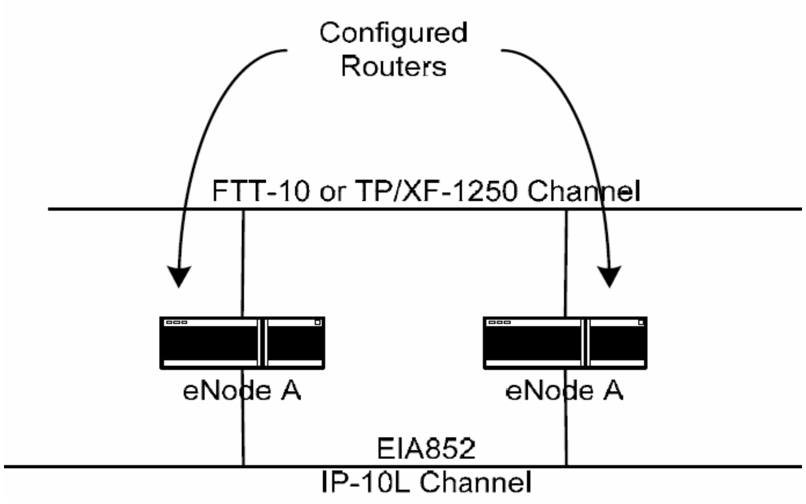
Router Types
- Configured Router
- Learning Router
- Bridging (Domain) Router
- Repeating Router

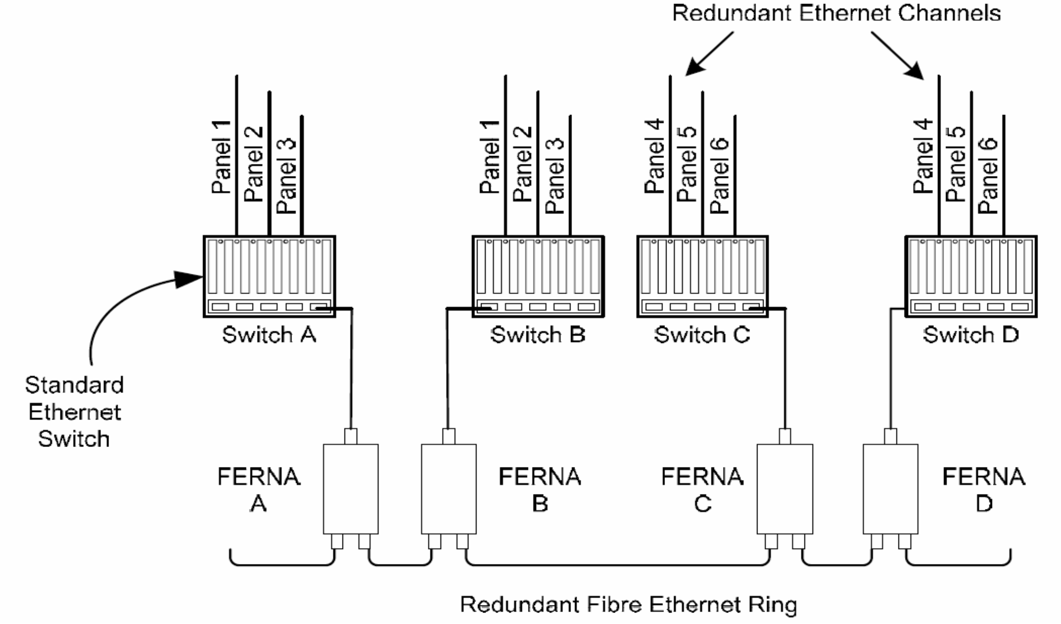
Staples Center

- Multi-event facility, Professional sports and concerts.
  - Opened in 1999
  - Original HVAC and smoke evacuation control system soon showed problems coping with operational demands
  - By 2004 Bill Pottorff, Director of engineering decided to replace control system with open interoperable approach to enable better performance, flexibility and future scalability
  - Replacement system based on 709.1 and 852
    - Leverages existing wiring and IP infrastructure
    - Allows multi-vendor equipment
    - Increases capability
    - Enables future expansion
  - Retrofit Team
    - Systems Integration, Infinite Control Systems
    - HVAC Controllers, Distech Controls
    - Adept Systems LON/IP Routers

Details


Field Devices - wiring in ring to allow connectivity on a break in the ring
eNode A
eNode B
EIA852 Monitoring
EIA 709.1 FTT-10 or TP/XF-1250
EIA709.1 Monitoring
To Switch A
To Switch B

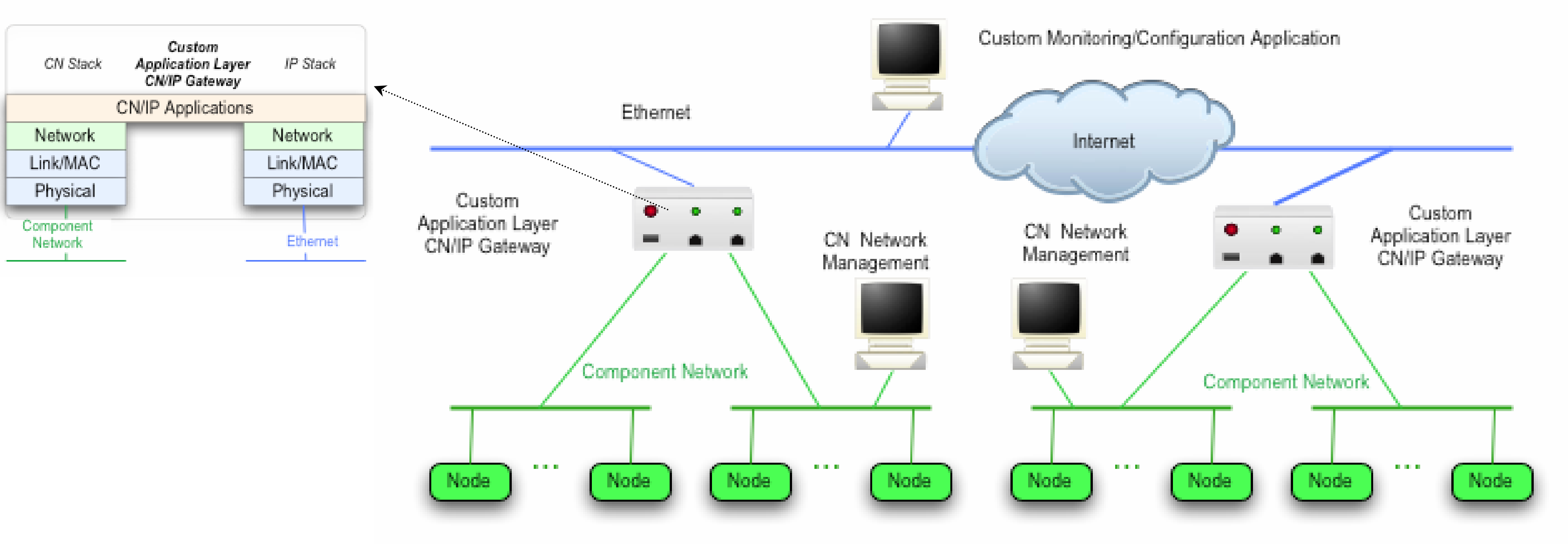

Configured Routers
FTT-10 or TP/XF-1250 Channel
eNode A
eNode A
EIA852 IP-10L Channel


Redundant Ethernet Channels
Panel 1
Panel 2
Panel 3
Panel 1
Panel 2
Panel 3
Panel 4
Panel 5
Panel 6
Panel 4
Panel 5
Panel 6
Switch A
Switch B
Switch C
Switch D
Standard Ethernet Switch
FERNA A
FERNA B
FERNA C
FERNA D
Redundant Fibre Ethernet Ring

IP Based Solutions

- Custom Application Layer Gateway:
  - CN to Custom IP Protocol
- Protocol Conversion Application Layer Gateway:
  - CN to Standard IP Protocol (BACNet, Others)
- Data Translation Application Layer Gateway:
  - CN to Internet Format (XML, HTTP,Soap others)
- 852 Open Standard Based CN/IP Router/Gateway
  - Transparent IP Backbone
  - High Availability Redundant Backbone
  - Flood Mode (Invisible Link)
  - NAT and DDNS

Custom Application Layer CN/IP Gateway



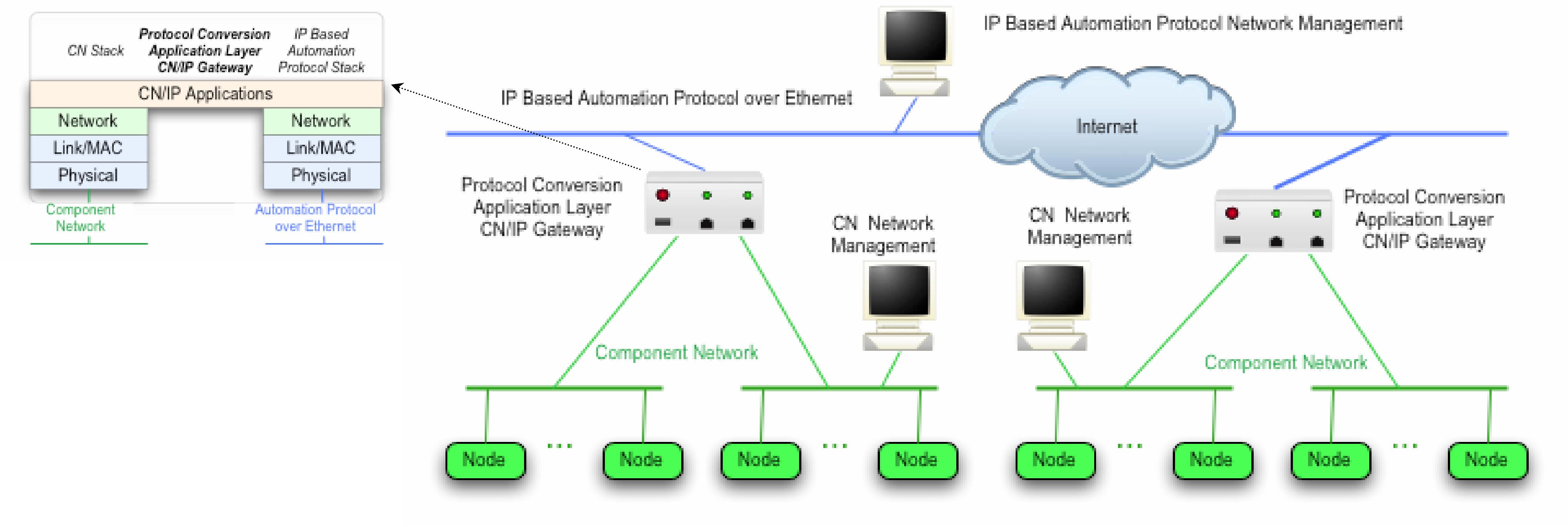
Advantages:

Swiss Army Knife
Logical Isolation - Proxy
Multiple-CN Protocols

Disadvantages:

Not Transparent From CN Perspective
Complicated Network Management
Proprietary - Non Standard
Performance Overhead
Host Application Limitations

Protocol Conversion Application Layer Gateway


CN Stack
Protocol Conversion Application Layer CN/IP Gateway
IP Based Automation Protocol Stack
CN/IP Applications
Network
Link/MAC
Physical
Network
Link/MAC
Physical
Component Network
Automation Protocol over Ethernet
IP Based Automation Protocol Network Management
IP Based Automation Protocol over Ethernet
Internet
Protocol Conversion Application Layer CN/IP Gateway
CN Network Management
CN Network Management
Protocol Conversion Application Layer CN/IP Gateway
Component Network
Component Network
Node
...
Node
Node
...
Node
Node
...
Node
Node
...
Node

Advantages:

Leverage Standard IP Protocol

IP Control Nodes

Logical Isolation - Proxy

Multiple-CN Protocols

Disadvantages:

Not Transparent From CN Perspective

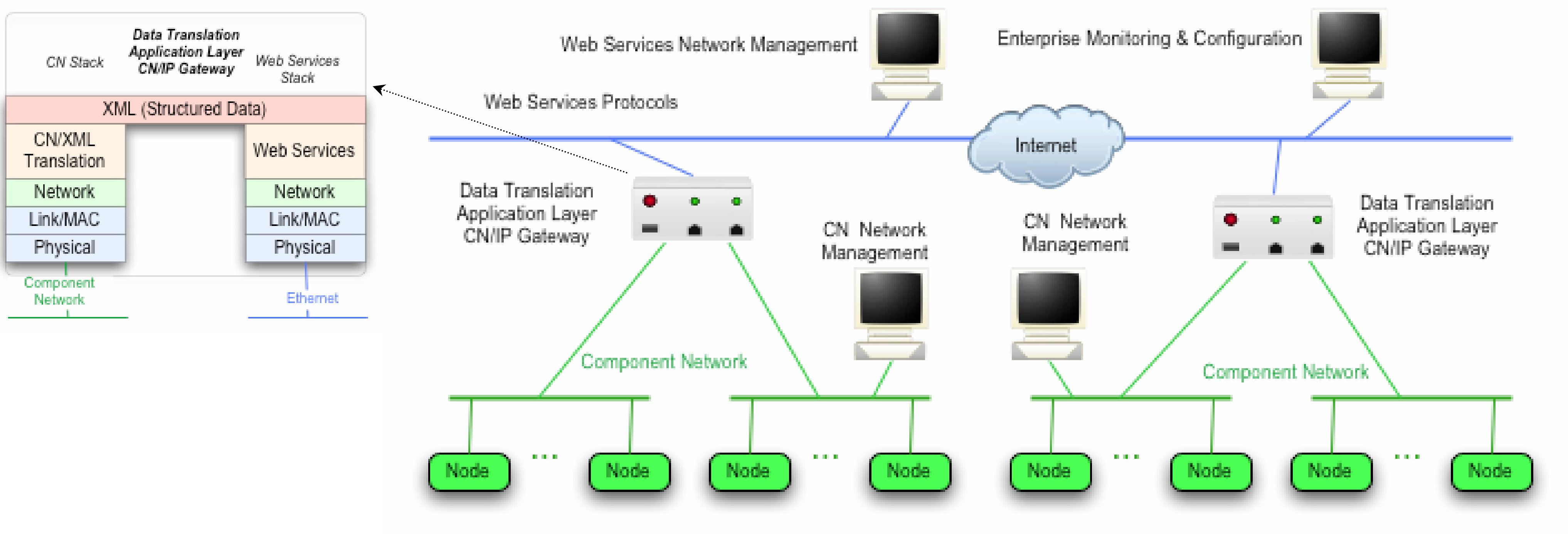
Complicated Network Management

Performance Overhead

Host Application Limitations

Data & Usage Mis-Matches

Data Translation Application Layer Gateway



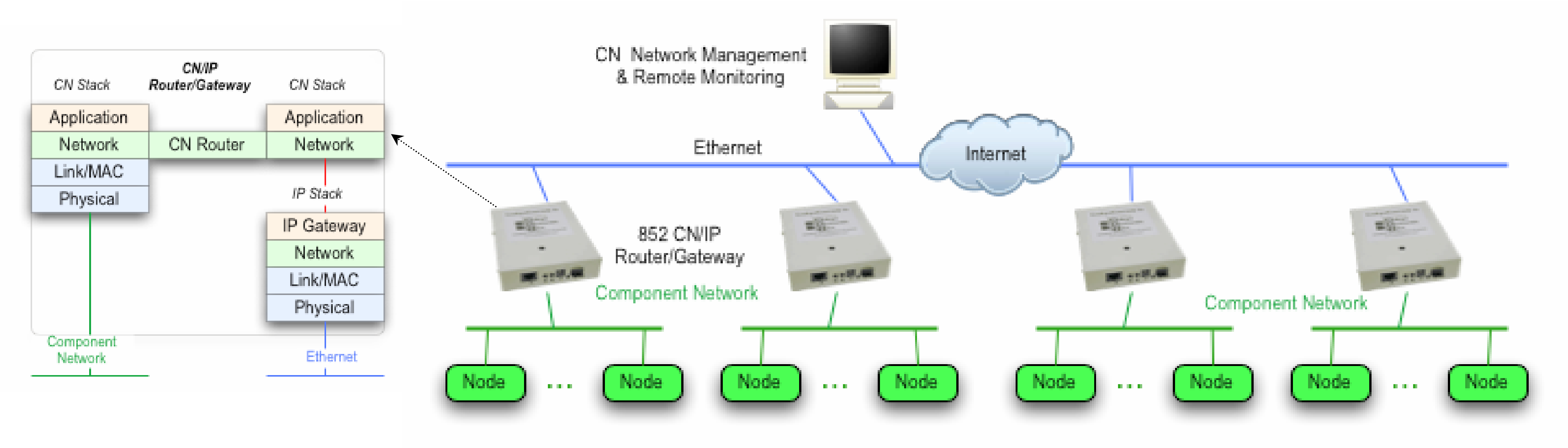
Advantages:

Leverage Web Services
Content Repurposing
Logical Isolation
Multiple-CN Protocols
Enterprise Integration

Disadvantages:

Not Transparent From CN Perspective
Complicated Network Management
Severe Performance Overhead
Host Application Limitations
Data & Usage Mis-Matches

852 Standard Based “Transparent” CN/IP Router/Gateway



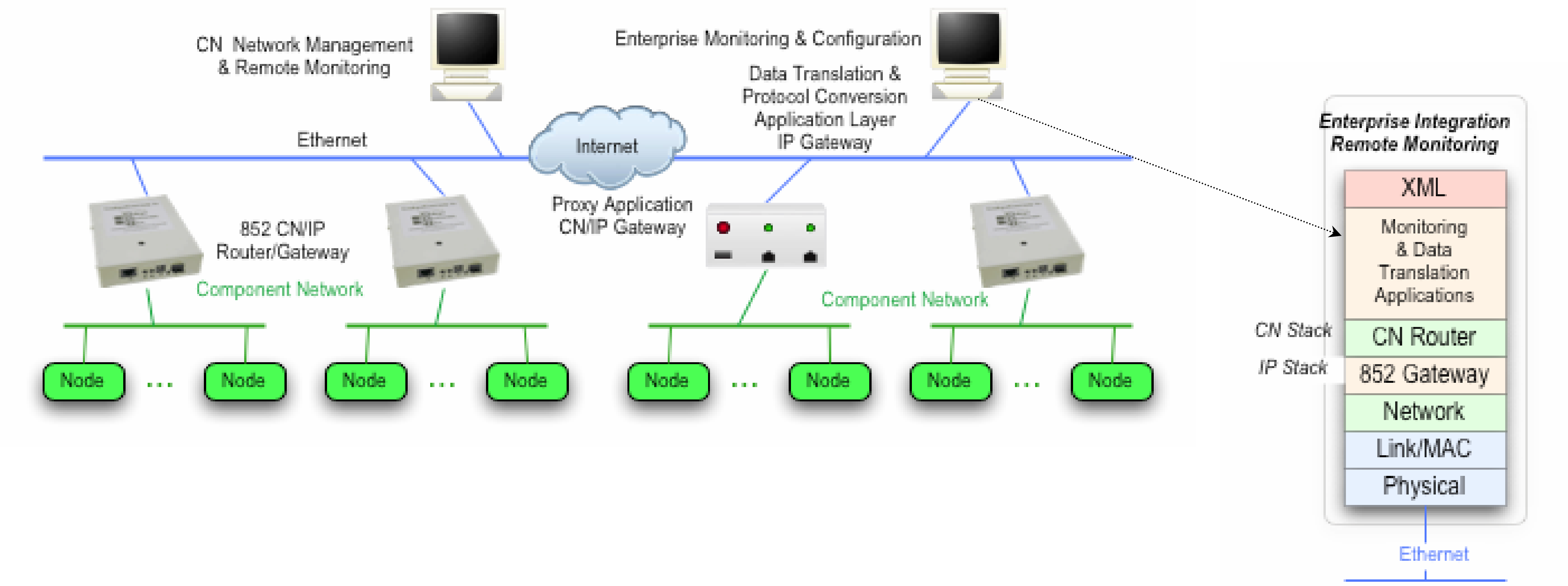
Advantages:

Transparent “Flat Architecture”
Unified Network Management
High Performance
Remote Monitoring
Enables Hybrid Architectures

Disadvantages:

No logical isolation
Single CN
No Data Translation

Hybrid Architecture



Advantages:

All

Disadvantages:

None

Critical Systems Infrastructure

- Transportation Systems: ships, trains, planes, bridges, highways
- Utilities: power plants, dams
- Public Facilities: stadiums, concert halls, amusement parks
- Large Office Buildings
- Telecommunications Centers
- Any Facility visited by large numbers of people

New Era for System Reliability

- New political environment has created an enhanced susceptibility to sabotage, terrorism, or other asymmetrical attack
- Eventual result will be new requirements and specifications for facilities with enhanced survivability aspects
- Conventional notions of reliability and systems design in the automation systems employed in many critical facilities do not account for catastrophic failure due to attack and hence are vulnerable.
- Homeland Security Needs: Affordable, Reliable, & Survivable Automation Systems

Baseline Technology Problem

- Historical building automation systems have not been robust to damage and do not provide *inherent cost-effective* survivability
- Open COTS automation technologies alone do not provide the inherent survivability needed for Homeland Security applications.
- ANSI 709.1/852 is the technology leader & de-facto open COTS standard for physical plant automation *but* survivability has not been a commercial priority.
- Adept has developed technology that enhances COTS automation technology to make it survivable and affordable.

Automation Infrastructure Attributes

- Scope = ubiquitous.
  - The infrastructure must include everything from the component level up through all the buildings subsystems, systems, operations, and off-site support.
- Access = transparent, peer-to-peer, global, & secure.
  - Transparency means that communication over the automation infra-structure's network is invisible to the application, that is, the overhead associated with network use is minimized.
  - The combination of peer-to-peer and global means that any given node can exchange information with any one node if so desired.
  - Secure means that all relevant information, sensor, control, & parametric data for each component are made available at appropriate levels of security.
- Structure = flexible.
  - The infra-structure must be scaled, extended, and adapted to different applications over space and time.
- Reliability = dependable.
  - Accurate media and network services must be continuously available at acceptable latencies.
- Cost = affordable.
  - The different attributes must be implemented in a highly cost effective manner. Reduced manning will only come at very high levels of automation with potentially thousands of nodes.
- Survivability = robust.
  - Must be capable of continued operation at sufficient levels of performance despite damage and casualties induced by shock, blast, fire, flooding, or radiation.

Fundamental Problem

- Commercial off the shelf approaches to automation infra-structures usually achieve some combination of attributes (1) - (5).

- What is unique to Homeland security applications is attribute (6), survivability. While many technology choices exist that may be able to provide attributes (1) - (4), the major difficulty in achieving a suitable automation infra-structure for Homeland security is providing both attributes (5) and (6), that is, affordability and survivability. Survivability is the major cost factor.

- Consequently, the key to the solution is in finding ways to achieve more cost-effective survivability.

Architecture Elements

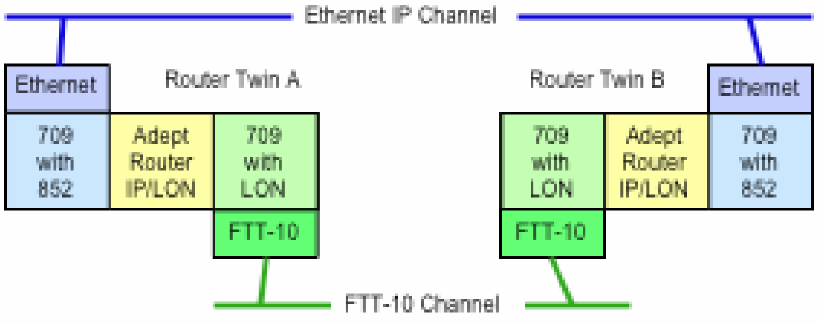
- Distributed intelligence: from the component level on up
  - Supervisory control with local autonomy in the event of fragmentation
  - Local intelligence provides enhanced survivability through local situation awareness and conditional response/behaviors
- Dependable partial mesh of channels topology
- Network fragment healing
  - Fine-grained online reconfiguration capability
  - Supporting electronics
- Network design, installation, configuration, & management tools
- Network early warning “pre-hit” pre-configuration tools
- Complementary survivable reconfigurable networked power system
- Threat simulation, analysis, training, evaluation, and role playing tools
- Neighborhood-wide integration

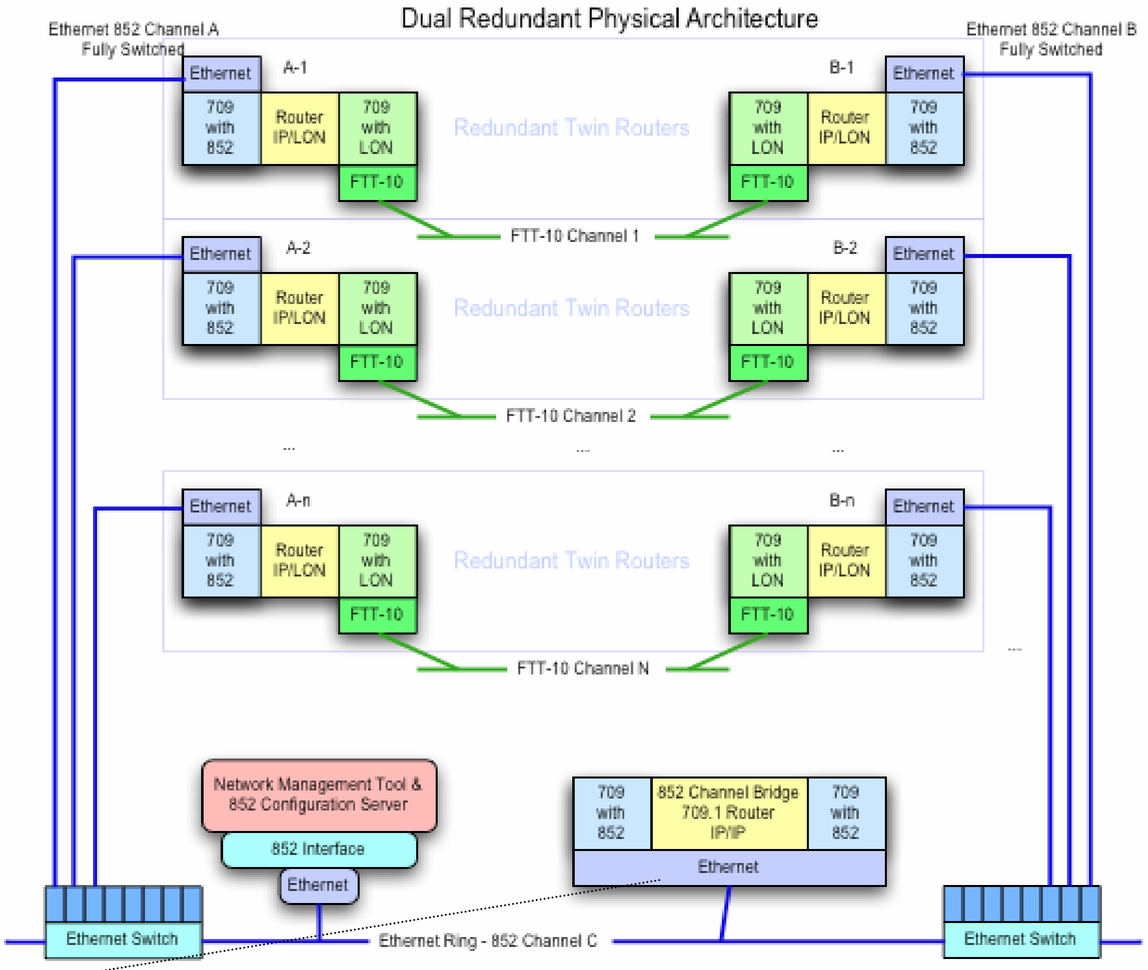
Elements and Applications

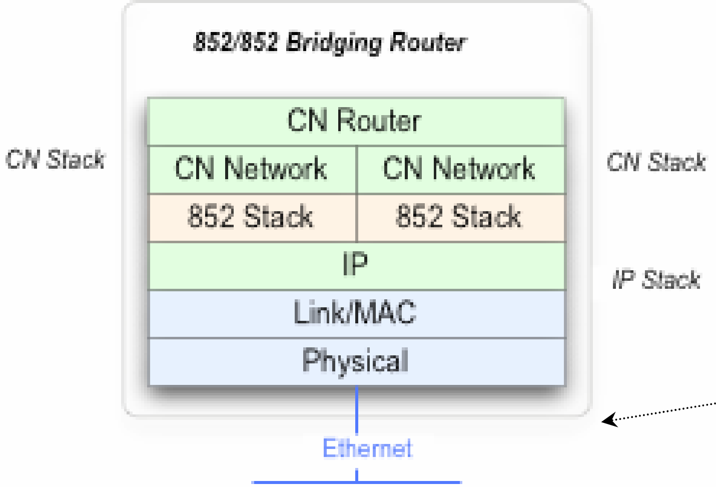
- Survivable automation infrastructure elements
  - Automation network:
    - media, sentinels, routers, and network power
  - Attached automated systems:
    - Controllers, sensors, actuators, and systems power
- Applications
  - Security, monitoring, and situational awareness
  - Evacuation management
  - Neighborhood coordination
  - Damage assessment, control
  - Condition based maintenance

High Availability Architecture

Dual Redundant CN/IP Routers


Ethernet IP Channel
Ethernet
Router Twin A
709 with 852
Adept Router IP/LON
709 with LON
FTT-10
Router Twin B
709 with LON
Adept Router IP/LON
709 with 852
Ethernet
FTT-10
FTT-10 Channel


Dual Redundant Physical Architecture
Ethernet 852 Channel A
Fully Switched
Ethernet 852 Channel B
Fully Switched
Ethernet
A-1
709 with 852
Router IP/LON
709 with LON
FTT-10
Redundant Twin Routers
B-1
709 with LON
Router IP/LON
709 with 852
Ethernet
FTT-10
FTT-10 Channel 1
Ethernet
A-2
709 with 852
Router IP/LON
709 with LON
FTT-10
Redundant Twin Routers
B-2
709 with LON
Router IP/LON
709 with 852
Ethernet
FTT-10
FTT-10 Channel 2
...
...
...
Ethernet
A-n
709 with 852
Router IP/LON
709 with LON
FTT-10
Redundant Twin Routers
B-n
709 with LON
Router IP/LON
709 with 852
Ethernet
FTT-10
FTT-10 Channel N
...
Network Management Tool & 852 Configuration Server
852 Interface
Ethernet
709 with 852
852 Channel Bridge 709.1 Router IP/IP
709 with 852
Ethernet
Ethernet Switch
Ethernet Ring - 852 Channel C
Ethernet Switch


852/852 Bridging Router
CN Stack
CN Router
CN Network
CN Network
CN Stack
852 Stack
852 Stack
IP
IP Stack
Link/MAC
Physical
Ethernet